IAPS REC'O PCTATO 30 MAR 2006

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY (SUPPLEMENTARY SHEET)

International application No.

PCT/EP2004/052243

10/574181

Re Box No. V

1 Reference is made to the following document:

D1: EP1076279

2 The present application does not meet the requirements of Article 33(2) PCT, because the subject matter of claims 1 and 10 is not novel.

2.1 Document D1 discloses:

Claim 1	Document D1
A method for granting an access to a	"controlling the installation and/or use of
computer-based object, wherein	data on computer platforms" (paragraph 1)
a memory card having a program code	"the platform may include a trusted
processor is provided, with at least one	module (smart card)" (paragraph 26)
public and one private key assigned to the	"the unlock key is encrypted by C
memory card being stored thereon,	(=third party) using the trusted module's
·	public key" (paragraph 69)
	"a trusted module stores a third party's
	public key" (paragraph 8)
an item of license information which	"the unlock key is used to allow the
comprises at least one license code	protected data to be decrypted and run
encrypted by means of the public key	using a public key infrastructure to encrypt
assigned to the memory card is provided at	a message containing an unlock key, and
a computing device controlling the access	checking for integrity via hashing and
to the computer-based object,	digital signatures" (paragraph 12, 37, 43,
	46, 56, 65-69)

"setting up shared symmetric keys
The sender generates a DES key - using a
random number generator, and making
sure these keys are only used once"
(paragraph 171)
"Both the data and the software executor
are hashed and signed with the
clearinghouse/developer's private key"
(paragraph 27)
· ,
"The secure loader integrity checks the
software executor when it is received"
(paragraph 27)
"Optionally, applications may be run
within a smart card." (paragraph 157)
"When the user wishes to run the data, the
secure executor decrypts the data using the
unlock key and allows the data to run."
(paragraph 160)
,

3 The independent claim 10 essentially corresponds to the method claim 1. The corresponding objections to claim 1 therefore apply also to the independent claim 10.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY (SUPPLEMENTARY SHEET)

International application No.

PCT/EP2004/052243

4 The dependent claims 2 to 9 also do not meet the requirements of Article 33 PCT, since they are neither novel nor inventive compared to D1.